PREPARED STATEMENT OF
THE NEW JERSEY STATE POLICE

Lieutenant Anthony W. Ritter
Assistant Bureau Chief
Computer Crimes and High Technology Surveillance Bureau

Before the

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

of the

COMMITTEE ON ENERGY AND COMMERCE

United States House of Representatives

July 10, 2006

Good morning Mr. Chairman, Ranking Member Stupak and members of the Subcommittee, I am Lieutenant Anthony Ritter, Assistant Bureau Chief of the Computer Crimes and High Technology Surveillance Bureau within the Special Investigations Section of the New Jersey State Police. I appreciate the opportunity to discuss with you our issues regarding combating predators on the Internet.

I. Introduction

I have been a member of the New Jersey State Police for 22 years and have been involved in both technology and cyber investigations for the last 17 years. The Computer Crimes and High Technology Surveillance Bureau which coordinates the efforts of the New Jersey Internet Crimes Against Children (ICAC) Task Force.

II. Challenges

I would like to address some of the challenges that face our task force and that of cyber law enforcement in general.

A. Data Retention

There has been much testimony before the committee on the subject of data retention by Internet Service Providers (ISPs) and I would like to address the three major concerns brought forth by ISPs generally. First, the ISPs are not clear who will be able to access records of someone's online behavior. The law enforcement process begins with reasonable suspicion to develop required probable cause and operates under legal guidance and court orders. I think unauthorized insider access to records is of graver concern to the ISPs. Second, the ISPs are not clear who would pay for the data warehousing of these additional records. I think everyone will bear part of the cost. And third, ISPs say it is not clear that police are hindered by current law as long as they move swiftly in the investigative process. In this case, they may be partly correct. There needs to be a consistent, measured approach to data retention and an increase in the speed of the investigative process. We both must work more efficiently. Although we are pleased to see the ISPs moving forward, voluntarily, to address our concerns where they can, we seek to have a standard established for the retention of data by ISPs. All ISPs should be required to have the capability of isolating targeted traffic and upon receipt of a court order, deliver that content to a law enforcement monitoring facility in a standardized manner. This capability needs to extend to all methods of communication services supported by this industry.

B. Quality of Service

Quality of service is an industry recognized term that is important to a business's ability to maintain and increase its customer base. In our case, law enforcement is the customer and poor customer service equates to a delayed law enforcement action. These delays can result in an inability to continue investigative leads in a timely manner. Our goal here is to institute industry wide standards to ensure the efficient and timely return of the information sought by law enforcement.

C. Costs

There is an explosion in technology and it is the convergence of telephony networks and data networks on portable data assistants (PDA), cell phones and other wireless devices. Current costs for intercepting conventional wireless devices can reach as much as $2600 per intercept order. Our fear is that the costs associated with IP intercept will exceed the costs of conventional intercepts and will price many law enforcement agencies out of this investigative crime fighting tool.

D. Personnel

The need for skilled investigators is as critical as data retention. Without the data we cannot investigate, without the detective we cannot investigate. In New Jersey's Peer-to Peer (P2P) initiative we have over 83,000 leads and as LTC Rodgers stated, we have 10 full time detectives with half working proactively. The other half are working reactively on referrals and direct complaints. And what about being proactive in other areas of the Internet? Most people only know of browsing the web, but there are many other ways of communicating across the Internet and each one could keep a whole squad of detectives busy 24 hours a day.

E. Tools

Additional research and development needs to be conducted by law enforcement, technology corporations, and institutions of higher learning to close the large gaps impeding our ability to fight technology crime against Internet predators. We need to:

- collect technical data and present it in an easy to view graphical format.
- automate the process of locating network log files regardless of operating system.
- overcome the obstacles of anonymizers, IP spoofing, encrypted data and steganography.
- forensically capture a computer's Random Access Memory (RAM) without modification or alteration.
- provide real time IP intercept on data networks in a standardized format, with the ability to isolate the target and capture the communication inclusive of all activities such as instant messaging, voice over IP phone calls, web cams, emails and web browsing.

- facilitate an automated and standardized stored data handover interface for the return of historical records requested by subpoena or court order.
- develop tools to locate the physical position of devices connected to wireless networks.

III. Solutions

There have been many suggestions from the men and women fighting Internet Crimes Against Children in New Jersey on ways to improve and streamline our mission. Here are some of their thoughts:

A. Increase ISP record retention to not less than two years to include, but not be limited to, subscriber information, method of payment, types of devices connected and all in and out IP logging records.

B. Mandate that out-of-state subpoenas and warrants be recognized as valid legal documents.

C. Create a website rating system much like the one used by the motion picture industry so that parents can more easily block content.

D. Sponsor a national Internet Safety campaign through television and movie theaters.

E. Evaluate the Counterdrug Technology Assessment Center's (CTAC) technology transfer program and model a similar program to support agencies combating Internet predators.

F. Recognize the FCC's *Second Report and Order and Memorandum Opinion and Order* that addresses several issues regarding implementation of the

Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994. The primary goal of the *Order* is to ensure that Law Enforcement Agencies have all of the resources that CALEA authorizes, particularly with regard to facilities-based broadband Internet Service Providers and interconnected voice over Internet Protocol (VOIP) providers. Although the VOIP issue has now been addressed, other packet based services such as instant messaging, picture messaging and a host of other Internet based communication services have been excluded from CALEA standards. This needs to be corrected.

G. Endorse, support and promote the expansion and implementation of Internet Protocol version 6 (IPv6) which will allow ISPs the ability to give every internet accessible device its own unique static IP address and eliminate the nightmare of dynamic IP addressing issues. The United States Government has specified that the network backbones of all federal agencies must deploy IPv6 by 2008.

IV. Conclusion

With the proper resources, states can and will do much more to continue the fight against Internet predators. We remain committed to maintaining existing operations without minimization and are honored to be a partner in the fight against Internet child victimization.

SUMMARY OF TESTIMONY

Lieutenant Anthony W. Ritter
Assistant Bureau Chief
Computer Crimes and High Technology Surveillance Bureau
New Jersey State Police

Before the
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
of the
COMMITTEE ON ENERGY AND COMMERCE
United States House of Representatives

July 10, 2006

1. Introduction
   a. 22 years law enforcement experience
   b. Oversees operation of the New Jersey Internet Crimes Against Children Task Force

2. Challenges
   a. Data Retention
      1) Need to establish standards for data retention
      2) Should apply to all methods of communication services
   b. Quality of Service
      1) Need for industry wide standards for return of information to law enforcement
   c. Costs
      1) Costs for intercept of data may prove prohibitive
   d. Personnel
      1) There is a serious lack of skilled investigators
   e. Tools
      1) Development of additional investigative technology tools is needed

3. Solutions
   1) Increase ISP record retention without limitations
   2) Recognition of out-of-state subpoenas and warrants
   3) Institute a website rating system
   4) Sponsor a national Internet Safety campaign
   5) Empower technology transfer programs to provide needed tools
   6) Expand CALEA to fully support all IP based communication services
   7) Support rapid deployment of IPv6